SECURITY AWARENESS NEWSLETTER

May 2002

In an effort to emphasize the importance of security issues to all staff and to promote security awareness, the GOT Division of Security Services will be providing monthly computer security alerts focused on practical tips, solutions, and job-saving techniques.

SECURITY POLICY AWARENESS

While most attention to network security has traditionally centered on tactical, preventive or reactive procedures--less emphasis has been given to examining the security policy itself and maintaining its operational health. The Division of Security Services is making an intentional effort to regularly update both GOT internal information systems security policies, as well as Enterprise standards and policies. In the near future, you will see several revised/updated and newly created security policies. As mentioned, some of these policies will be internal standards for core business security practices within GOT, while other policies will apply to agencies outside of GOT and will be considered Enterprise Policies and Procedures. GOT staff are encouraged to familiarize themselves with all security policies and procedures, especially those that have been recently updated and created.

Back to Top

HOMELAND SECURITY ACTIVITIES

According to Ray Nelson, Executive Director, Office for Security Coordination of Homeland

Security, a basic and fundamental role of government under our constitution is to protect Americans from both foreign and domestic threats. Mr. Nelson will work closely withthe newly-created federal Homeland Security Office, headed by former Pennsylvania Governor Thomas Ridge. For more information, see http://techlines.state.ky.us/homeland.htm.

Listed below are some of the "post 9/11" activities being done by the Commonwealth of Kentucky and GOT:

- A Homeland Defense Team was created, which consists of cabinet secretaries of major state agencies having responsibility related to the overall support of state government.
- An Inter-Agency-Safety-Security Team has been created, which consists of similar agencies as the Homeland Defense Team, and they are working on operational issues such as security awareness, disaster recovery, etc.
    - Videos are being produced to help state employees learn how to handle certain circumstances, whether a natural disaster,bioterrorism, etc.
- Physical Security Enhancements of GOT Facilities.
- Improvements are being made in firewall monitoring and intrusion detection systems to help better serve our customers.

Some long-term implications for Kentucky will be addressed at the Kentucky Long-Term Policy Research Center's ninth annual conference, which will be held November 21, 2002, at the Executive Inn Rivermont, in Owensboro. The conference will address several issues related to "9/11," such as public health, technology, the economy, agriculture, tourism, government, the military, and others. See http://www.kltprc.net/conference2002.htmfor more information.

Back to Top

CREATIVITY USED BY SOCIAL ENGINEERS

Creativity is not always a "good" thing. More often than you might think, someone applies a little creativity to obtain valuable information without having to break into a computer or building. These resourceful individuals are known as "social engineers," and they will try to con you into divulging information that you normally would not share. This could be confidential information, credit card numbers, system passwords, and more. Most social engineers prefer to use the telephone for their information gathering in order to protect their anonymity. Some will dig through the trash looking for discarded (but important) information. Believe it or not, a determined social engineer will go as far as entering an office using the uniform of a repairman or other figure commonly seen in a place of business.

It is important to recognize the signs of a social engineering attempt. To avoid getting caught, the social engineer may provide false or vague contact information. Often, they will express a sense of urgency to get you to act quickly so that you provide information without properly verifying their request. These con artists count on your natural desire to help others. But beware--what may seem like an innocent request could be an elaborate trick designed to get confidential information.

By asking questions to validate the request, you can help protect yourself and our information. When pressed for answers, a social engineer will usually abandon his or her effort. **Be creative yourself** by applying these tips to turn the table on a social engineer:

- Ask who has authorized the request.
- Verify the authorization.
- Confirm the identity of the requestor.
- Ask for and verify complete contact information.
- Inquire as to why the information is needed.
- Never give information about your network over the phone or via email. Hackers can use such information to exploit vulnerabilities.
- Be wary of unescorted visitors.
- Seek assistance if in doubt.
- Report any suspected social engineering attempt by completing GOT-F012, which can be found at http://www.state.ky.us/got/ois/security/Security_forms.htm
- And never tell anyone your password under any circumstances.

Back to Top

PASSWORDS

Passwords truly are the keys to our data. If someone with malicious intent is able to obtain password(s) and get confidential data, it can be very disastrous. All a hacker needs is one password; with that they usually have all they need to start to break through all the security the systems administrators have put together. Hackers also have password cracking programs that'll take minutes to crack passwords that aren't properly constructed. If it's worth it, they'll spend hours, even days, running passwords through these programs in order to break one.

You may think this is all a little overboard, but it's important that we, as the holders of the keys, learn to take the proper care with our passwords just as we have with other types of keys. You would probably never think of lending someone your key or pass card to get into your office building. You'd certainly never give someone else your bank PIN number. Passwords need to be thought of in a similar way; a lot is at stake if the password falls into the wrong hands.

Back to Top

VIRUS INFORMATION / MCAFEE PROTECTION and WEBCASTS

According to McAfee, over 60,000 known viruses roam the virtual world, in addition to untold quantities of insidious Java, ActiveX, and JavaScript.

During the last three months, SirCam and Magistr were the most popular viruses/worms seen coming in through the Internet. A medium alert was issued by McAfee on a variant of W32/Klez, which takes advantage of vulnerabilities in unpatched Internet Explorer and Outlook Express software. The major difference is that Klez.H has the apparent ability to spread more widely. McAfee's 4182 DAT protects against this variant.

GOT continues to encourage a multi-tiered approach to anti-virus protection. It is essential that each user has updated anti-virus software on their desktop as the first level of anti-virus defense, and that the software is configured to get the latest DATs and engines on a timely basis. GOT is taking this measure as well as doing everything possible to be sure that other bases are covered by protecting the gateway, protecting the servers, and thus protecting the users.

Our site license with McAfee includes a home use option for all participants (at no additional charge). Home users should be sure that they have adequate virus software installed on their home computers. They should check with their Cabinet McAfee designated level representative for additional information. These contacts are listed on the state's anti-virus website at http://www.state.ky.us/got/ois/security/antivirus.

For GOT staff members, Shawn Thomas, GOT Virus Defense Team, created an e-mail distribution list that includes GOT staff who participate in the Home/Laptop Virus Protection Program. Each week, the latest DATs, as well as the URL for downloading them, are e-mailed to GOT staff unable to receive attachments via email.

For more information about McAfee and its products, see their WebCasts, which are offered every Tuesday, Wednesday and Thursday. Log on to experience product demonstrations and ask questions in a Q & A session. **No pre-registration is required**. See http://www.mcafeeb2b.com/products/live-webcasts.asp

Back to Top

HOAXES/CHAIN LETTERS

According to McAfee, while there are a lot of viruses out there, there are some viruses that aren't really out there at all, such as virus hoaxes. Hoax virus warning messages are more than mere annoyances. After repeatedly becoming alarmed, only to learn that there was no real virus, computer users may get into the habit of ignoring all virus warning messages, leaving them especially vulnerable to the next real, and truly destructive, virus.

Fortunately, McAfee tracks virus hoaxes as well as genuine viruses. The next time you receive an urgent virus warning message, check it against the list of known virus hoaxes below. If it's a hoax, chances are you'll find it in their database. And if it's a real virus, they'll probably know about it already, and you'll find it in McAfee's Virus Information Center at http://vil.nai.com/VIL/newly-discovered-viruses.asp. A list of known virus hoaxes can be found at http://vil.mcafee.com/hoax.asp.

For more information, take a look at the "Virus hoaxes are more than mere annoyances" article on GOT's security web site athttp://www.state.ky.us/got/ois/security/breaking.htm

Chain letters have the same purpose as hoaxes but use a slightly different method of getting you to forward them on to everyone you know. They usually promise a phenomenal return on a small effort. The simplest form of a chain letter contains a list people in which you're asked to forward to the top person on that list. You then remove the top person on the list, sliding the second person into the top position, and add yourself in the bottom. You usually are requested to forward the chain letter on to your friends, with a promise that you will eventually receive *"something"* in return.

However, chain letters are illegal and a waste of time; they have the potential for wasting great amounts of bandwidth and disk space; and they are in violation of the Commonwealth of Kentucky's Internet and Electronic Mail Acceptable Use Policy, which can be found at http://www.gotsource.net/dscgi/ds.py/View/Collection-1450.

Back to Top

CREATOR OF "MELISSA" GETS 20 MONTHS

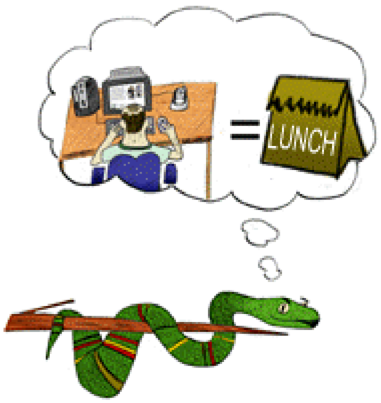
One of the first people ever prosecuted for creating a computer virus, "Melissa," creator David L. Smith, 33, was sentenced Wednesday, May 1, to 20 months in federal prison for causing over $80 million dollars of damage in 1999 by disrupting e-mail systems worldwide. According to an Associated Press report, "Smith could have faced up to five years in prison, but prosecutors suggested a term of about two years, saying he had given authorities extensive assistance in thwarting other virus creators."

For more information, see http://www.cnn.com/2002/TECH/internet/05/01/melissa.virus.ap/index.html.

Back to Top

FEATURED ARTICLE FROM THE STATE OF IOWA

Anyone can become prey. Please be aware that there are hackers out there that don’t care



who you are or what you are doing, you are simply a target to them. Like a very hungry carnivore in the jungle, they will eat you if they get the chance. Be mindful that some people are even using the Sept. 11 tragedies and associated issues to lure you to their sites in order to compromise your systems or to get credit card numbers to steal your money.

Remember that many bad things from the Internet jungle are contagious. The 1i0n worm, reputed Chinese hackers, and Russian credit card thieves are all examples of real threats. (Lions and Tigers and Bears, oh my!) If you get infected with a worm or virus, or a bad critter compromises your system, it could dramatically - and badly - affect your agency's network as well. In protecting your own system you are also protecting the state's network

Thanks for your time, and be careful– it's a jungle out there!

Written by William Hubbard, Information Technology Department, State of Iowa
Artwork by Sam Wong, Information Technology Department, State of Iowa

Back to Top

ADMIN, DOMAIN ADMIN, AND NORMAL WORKSTATION ACCOUNTS

In the course of examining environments and talking with administrators, there are many examples of cases where the Administrator account and the Domain Admin group are misused. All too often, the only requirement for having access to the admin account is to be in a member of the IT department, which opens up many security holes.

Some Best Practices with Regards to the Administrator Account:

- Rename it.
- Passwords should be very complex.
- Create a new admin account with a complex password, disable it, and audit events on the network for attempted uses of the new "Administrator" account.
- Limit access to the Admin account to one or two people.
- Write down the Admin account information on a card, seal it in an envelope, and lock it in a properly controlled safe. This will ensure retrieval.

Some Best Practices with Regards to the DomainAdmins:

- Limit membership to a few highly trusted accounts.
- Members should have other accounts that they use for everyday business.
- Use the Account Operator, Server Operator, Backup Operator, and Print Operator groups for the Help Desk and other networkadmins.
- Grant special rights to other groups only when needed.

- Ensure that service accounts are not part of DomainAdmins.

Some Best Practices with Regards to the Normal Workstation Accounts:

- The Local Admin account should be renamed with a complex password.
- Besides the Domain Admin group, only add the main user of the workstation to the Administrator group (if necessary).
- The Guest account should be renamed with a complex password and should be disabled until needed.

Keep in mind that some viruses are stopped from doing severe damage because the user context that the task is run in does not have sufficient privileges or rights.

Back to Top

MICROSOFT UPDATES

Microsoft released Baseline Security Analyzer (MBSA) on April 8, 2002, which analyzes Windows systems for common security misconfigurations or problems--such as when computers are set up incorrectly or users fail to install suggested patches. Version 1.0 of MBSA includes a graphical and command line interface that can perform local or remote scans of Windows systems. MBSA runs on Windows 2000 and Windows XP systems and will scan for missing hotfixes and vulnerabilities in main Microsoft's products. For more details, see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsa

Finjan Software points out a flaw in MBSA and has issued an alert describing a security vulnerability in MBSA. Also, GOT has found reporting inconsistencies in it, and would not advise that it be the only tool used. While the tool offers a good service, it generates a report in plaintext that can be misused by crackers to exploit the vulnerabilities listed. For more information, see http://www.finjan.com/mcrc/alert_show.cfm?attack_release_id=71

Windows Update Corporate Edition, which Microsoft plans to release in the second quarter of 2002, will let administrators host their own version of the Windows Update Web site on a local intranet. Windows Update Corporate Edition will, at scheduled intervals, pull the latest fixes from the public Windows Update Web site. A client component will let administrators check the intranet-based Windows Update site and use Group Policy settings to automatically download updates to clients.

The Windows Update Corporate Edition will help companies preserve bandwidth that they now use to repeatedly download the same fixes and will offer greater control over which updates users can install. More information can be found at Microsoft's site at http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/ittasks/support/corpwu.a

Microsoft also recently released its first security rollup package for Windows NT Server 4.0, Terminal Server Edition (TSE SRP1). The rollup includes the functionality of virtually all security patches since the release of TSE service pack 6. Eight patches that missed the production cut-off date are listed in the bulletin. More information can be found at http://www.microsoft.com/technet/security/news/nt4tsesr.asp

Back to Top

CRITICAL INTERNET SECURITY VULNERABILITIES

According to Gartner, through 2005, 90 percent of cyber attacks will continue to exploit known security flaws for which a patch is available or a preventive measure known. Patches were available to protect systems against the "Code Red" worm, but had generally not been deployed, and the "Nimda" virus exploited exactly the same weakness a few months later and was still able to cause havoc around the world. Combined losses from the two incidents are estimated at running into billions of dollars.

It is only a matter of time before another Code Red or Nimda worm attacks. These worms have multiple modes of attack and infection. They also have been known to be polymorphic (can take many forms) and to plant Trojan horses on infected machines. The worms are also getting harder to eradicate and re-invention is becoming more prevalent.

Denial of Service (DoS) attacks are a very serious problem, and GOT has seen an increase in DoS attacks from the internet aimed at state systems. The worst aspect of these attacks is that there is very little that can be done to stop an attack, except blocking the traffic from the internet. The attacks cause congestion of the local network and Internet traffic by using available bandwidth. When access from the internet is blocked, legitimate internet traffic is also hindered.

Warez sites (sites containing unauthorized storage of illegal software) are a big problem due to the insistence some have to employing anonymous FTP. GOT is still finding warez sites and there are probably more within the state. This illegal use of state resources increases the Commonwealth's liability since it is responsible for what happens on its servers. Also, the existence of these sites brings visitors to our environment that we do not desire, and we will continue to be on the look-out for them.

The last defacement mirror site went off-line recently. During the period it was down, defacements seemed to diminish. The site has since solved its problems and is back in business. While the site still appears to be experiencing some problems, reported defacements are returning to levels similar to those before the site went offline.

Back to Top

USEFUL URL's

http://www.fedcirc.gov/

The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security-related issues affecting the civilian agencies and departments of the federal government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense (DOD), Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments forming a multi-talented virtual security team.

http://www.infosecnews.com/

This on-line news service is backed by SC Magazine - the largest circulation information security magazine. It is read in more than 50 countries around the world and is published in three separate editions in North America, Europe and the Asia Pacific region. The news service gathers information globally through a network of correspondents and over 200 news services. Key links associated with the news direct you to further sources of information relevant to the news item being reported.

http://www.zdnet.com/

ZDNet operates a worldwide network of Web sites for people who want to buy, use, and learn about technology. Winner of the Computer Press Association's "Best Overall Site" award for two consecutive years,ZDNet provides an invaluable perspective and resources for technology decision makers to gain an edge in business.

http://www.searchsecurity.com/

SearchSecurity.com is the home of TechTarget, offering the most targeted media for enterprise IT professionals, including industry-specific web sites, more than 100 e-mail newsletter titles, print media, exclusive, invitation-only conferences, live online events and list rentals.

http://www.computerworld.com/

Computerworld continually provides IT leaders with a host of targeted information services including their award-winning newspaper, web site, email newsletters, events and books. What's more, they provide unmatched reach to IT leaders with targeted advertising and sponsorships.

www.incidents.org

Incidents.org is a virtual organization of advanced intrusion detection analyst experts and forensic incident handlers from across the globe. The organization's mission is to provide real time driven security intelligence and support to both organizations and individuals.

www.sans.org

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face.

Back to Top

Works Cited

A portion of the material in this newsletter was authored by Kenton Smith,GIAC certification candidate as part of his certification process with the SANS Institute.